REPUBLIC OF SOUTH AFRICA

REPUBLIEK VAN SUID AFRIKA

PATENTS ACT, 1978

CERTIFICATE

In accordance with section 44 (1) of the Patents Act, No. 57 of 1978, it is hereby certified that

ACRES GAMING INCORPORATED

has been granted a patent in respect of an invention described and claimed in complete specification deposited at the Patent Office under the number

2004/7452

A copy of the complete specification is annexed, together with the relevant Form P2.

In testimony thereof, the seal of the Patent Office has been affixed at Pretoria with effect from the **25th** day of **May 2005**

.....

Registrar of Patents

FORM P.2

REPUBLIC OF SOUTH AFRICA | REGISTER OF PATENTS | PATENTS ACT, 1978

OFFICIAL APPLICATION	LODGING DATE: PROVISIONAL	ACCEPTANCE DATE
21 01 2004/7452	22	47 16.3.05
INTERNATIONAL CLASSIFICATION	**LODGING DATE: COMPLETE**	**GRANTED DATE**
51 G06F	23 16 SEP 2004	25-5-05

FULL NAME(S) OF APPLICANT(S)/PATENTEE(S)

71 ACRES GAMING INCORPORATED

APPLICANTS SUBSTITUTED:	DATE REGISTERED
71	

ASSIGNEE(S)	DATE REGISTERED
71	

FULL NAME(S) OF INVENTOR(S)

72 COPPERT, MICHAEL P

PRIORITY CLAIMED	COUNTRY	NUMBER	DATE
N.B. Use International abbreviation for country (see Schedule 4)	33 NIL	31 NIL	32 NIL

TITLE OF INVENTION

54 METHOD AND APPARATUS FOR MONITORING AND UPDATING SYSTEM SOFTWARE

ADDRESS OF APPLICANT(S)/PATENTEE(S)

7115 AMIGO ST, SUITE 150, LAS VEGAS, 89119, NEVADA, UNITED STATES OF AMERICA

ADDRESS FOR SERVICE	S & F REF
74 **SPOOR & FISHER, SANDTON**	PA138104/ZA

PATENT OF ADDITION NO.	DATE OF ANY CHANGE
61	

FRESH APPLICATION BASED ON	DATE OF ANY CHANGE

SPOOR & FISHER

FORM P.7
(To be lodged in duplicate)

REPUBLIC OF SOUTH AFRICA
PATENTS ACT, 1978

COMPLETE SPECIFICATION

(Section 30(1) – Regulation 28)

OFFICIAL APPLICATION NO.			LODGING DATE	
21	01	2004/7452	22	16 SEP 2004

INTERNATIONAL CLASSIFICATION	
51	G06F

FULL NAMES OF APPLICANT	
71	ACRES GAMING INCORPORATED

FULL NAMES OF INVENTOR	
72	COPPERT, MICHAEL P

TITLE OF INVENTION	
54	METHOD AND APPARATUS FOR MONITORING AND UPDATING SYSTEM SOFTWARE

METHOD AND APPARATUS FOR MONITORING AND UPDATING SYSTEM SOFTWARE

FIELD OF THE INVENTION

This invention pertains to monitoring software for a variety of conditions such as internal performance characteristics, liability warnings, programmatic errors and the general health of the computer system.

BACKGROUND OF THE INVENTION

No matter the computer program, it is inevitable that there will be some bugs (that is, coding errors that cause the program to behave differently what is expected). Production environments represent a number of variables that are difficult to reproduce in testing environments. As such, applications with thousands of interfaces can fail under a variety of changing variables.

Because human intervention is required to maintain these applications, certain tasks must be completed by operations on a timely basis. Failure to operate and maintain the system within the published guidelines for the application will result in a number of unacceptable issues. These include, but are not limited to the following: inaccurate reporting of revenues; increased risks associated with liability; increased risks with system availability; and increased costs due to additional manpower correction activities.

Customers want to know that their mission critical system is performing at peak levels of performance. They want to know when an area of the system is failing. They need to feel confident that the system and its integration with operations are running smoothly. Not knowing the health of the internal components of the system can create a false sense of security.

Another thing software companies sometimes do to eliminate defects is to find out about defects from customers. For a long time, customers had to make contact with the software companies (either by telephone or by e-mail) and let the software companies know about the bugs. More recently, as exemplified by Microsoft® Windows® XP, the operating system offers to send an error report to the software company when a program crashes. That

way, the software company is informed about serious errors. (Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and other countries.)

Some third party products that monitor the operation of systems from the outside exist. For example, Netcool, by Micromuse, collects information from APIs, log files, and other utilities, and forwards this information to a server for filtering. Patrol, by BMC Software, offers remote monitoring and full-application management. But both of these products are external to the applications being monitored. These products focus primarily on external environments surrounding the application. They cannot detect the internal health of the application itself and thus their reporting value is limited in scope.

A need remains for a way to proactively detect application problems and software defects through monitoring internal application performance beyond that associated with the prior art.

SUMMARY OF THE INVENTION

The invention is an apparatus, system, and method for monitoring computers. A series of probes residing on a customer's computer determines values for metrics and sends these values to a monitoring apparatus. The monitoring apparatus determines if the values for the metrics are acceptable. If the values for the metrics are not acceptable, then an alert is displayed so that a corrective measures can be initiated.

The foregoing and other features, objects, and advantages of the invention will become more readily apparent from the following detailed description, which proceeds with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows a central server with a monitoring apparatus, communicating with probes on customer computers, according to an embodiment of the invention.

FIG. 2 shows details of the monitoring apparatus of FIG. 1.

FIG. 3 shows details of the probes of FIG. 1.

FIG. 4 show the probes of FIG. 1 communicating with the monitoring apparatus of FIG. 1.

FIG. 5 shows a flowchart of the procedure for using the probes of FIG. 1.

FIGs. 6A-6C show a flowchart of the procedure for using the monitoring apparatus of FIG. 1.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. 1 shows a central server with a monitoring apparatus, communicating with probes on customer computers, according to an embodiment of the invention. In FIG. 1, server 105 is a central server. Server 105 is operated by the company distributing software products to its customers. Customers operate, for example, computers 110, 115, and 120. Although a person skilled in the art will recognize that there can be more or fewer than three customers, and that each customer can have more than one computer.

Installed on computers 110, 115, and 120 are probes 125, 130, and 135. Probes 125, 130, and 135 are responsible for determining the values associated with various metrics on computers 110, 115, and 120 respectively, and transmitting these values back to server 105. The details of probes 125, 130, and 135 are discussed further with reference to FIGs. 3-4 below.

Server 105 includes monitoring apparatus 140. Monitoring apparatus 140 receives information from probes 125, 130, and 135, and determines whether the data received from the probes represent acceptable values. If the values are acceptable, then monitoring apparatus 140 logs the values. Otherwise, monitoring apparatus displays 140 an alert, indicating the unacceptable value. The details of monitoring apparatus 140 are discussed further with reference to FIG. 2 below.

Connecting server 105 with computers 110, 115, and 120 is network 145. Network 145 can be any variety of network including, among others, a local area network (LAN), a wide area network (WAN), a global network (such as the Internet), and a wireless network (for example, using Bluetooth or any of the IEEE 802.11 standards). In addition, a person skilled in the art will recognize that different networks can be used to connect server 105 with different computers. For example, server 105 might be connected to computer 110 using one network, and to computers 115 and 120 using a second network.

FIG. 2 shows details of the monitoring apparatus of FIG. 1. Monitoring apparatus 140 includes four components: receiver 205, tester 210, alerter 215, and log 220. Receiver 205 is responsible for receiving a message from a probe and parsing the message for the necessary information. Tester 210 then tests the value (or values) retrieved from the message received by receiver 205 to determine if the value is acceptable. Alerter 215 displays an alert is the value retrieved from the message is not acceptable. And log 220 includes entries, like

entry 225, which reflect the received message, its values, and/or whether the value is acceptable.

To determine whether a value is acceptable, monitoring apparatus 140 uses database 230. Database 230 includes filters, such as filters 235, 240, and 245, which identify what values are considered acceptable. Different filters exist for different metrics. For example, filter 235 is a filter for the number of transactions occurring at a given location, whereas filter 245 is a filter for the number of open days experienced at a location.

Some filters, such as filter 245, can be used for all casino locations. But other metrics, such as the number of transactions, can vary from one location to another. To account for differing interpretations of acceptable values, different filters can be set up for a single metric, each filter identifying acceptable values for a different casino location. Thus, while filters 235 and 240 both represent acceptable values for the transactions metric, they represent acceptable values for different casinos.

Although a different filter can be set up for each different site for a given metric, the amount of variation in acceptable values might be limited. Where two or more sites agree on what constitutes an acceptable value for a given metric, there is no need for each site to have a separate filter. Thus, while FIG. 2 shows filters 235 and 240 being used for individual sites, a person skilled in the art will recognize that a single filter can be used for some (but not necessarily all) sites.

To select the appropriate filter, monitoring apparatus 140 uses selector 250. Selector 250 uses information from the message to select the appropriate metric. Selector 250 determines the metric represented in the message and, if necessary, the site from which the metric was measured. Selector 250 then uses these pieces of information to find the appropriate filter in database 230, so that tester 210 can determine if the value is acceptable.

FIG. 3 shows details of the probes of FIG. 1. In FIG. 3, probe 125 includes sensors 305, 310, and 315. Each sensor operates to determine values for different metrics for computer 110. For example, sensor 305 determines the number of transactions that occur in a given day in database 320 on computer 110, sensor 310 determines the number of open days at the site, and sensor 315 determines the number of fixes applied to software 325 on computer 110. A person skilled in the art will recognize that although three sensors are shown within probe 125, there can be fewer or more sensors in a given probe. In addition, there can be more than one probe for a given computer, each with the same or differing numbers of sensors.

Because sensor measurements are taken more than once, each of sensors 305, 310, and 315 includes a corresponding timer 330, 335, and 340. The timers ensure that the sensors take measurements according to regular schedules. Each timer can be set to measure a metric using different intervals. But a person skilled in the art will recognize that, for sensors measuring metrics according to consistent schedules, a single timer can be used for more than one sensor.

Additionally, sensors can trigger on two different mechanisms. They can be triggered on a timer or they can be triggered by an impromptu event. The latter is utilized to signal immediate attention to a critical event that has just taken place.

Finally, probe 125 includes message generator 345. Message generator 345 takes the measurements from the various sensors 305, 310, and 315, and assembles a message from the measurements. The message is then sent to the central server (not shown in FIG. 3). Message generator 345 can generate a single message for several metric measurements, or message generator 345 can generate a separate message for each metric measurement.

FIG. 4 show the probes of FIG. 1 communicating with the monitoring apparatus of FIG. 1. In FIG. 4, message generator 345 is shown generating message 405. Message 405 is shown in greater detail in blow-up 410. The message is dated August 7, 2003, and is from site 1 (which includes computer 110). Blow-up 410 shows two metric measurements. The site has measured 500,000 transactions, and has five open days. There can also be other metrics included in the message.

Once message 405 is generated, it is delivered to e-mail server 415. E-mail server is responsible for starting message 405 along its journey to receiver 205 in the central server. Although shown as a component of computer 110, a person skilled in the art will recognize that e-mail server 415 can be part of a separate computer, distinct from computer 110, or can be a dedicated e-mail server. A typical implementation would most likely utilize the customer's existing e-mail implementation. This will provide a number of benefits including a cost savings through the elimination of a second server along with cost avoidance of supporting and maintaining the additional hardware.

FIG. 5 shows a flowchart of the procedure for using the probes of FIG. 1. At step 505, the probe accesses a value for a metric. The value can be accessed from a database or from software. As shown by arrow 510, step 505 can be repeated as often as necessary, to access values for multiple metrics. At step 515, a message is generated. At step 520, the message includes the value for the metric accessed in step 505. At step 525, the site is

included in the message, so that the central server knows from where the message originated. At step 530, the message is delivered to the e-mail server, and at step 535, the message is sent to the monitoring apparatus by the e-mail server.

FIGs. 6A-6C show a flowchart of the procedure for using the monitoring apparatus of FIG. 1. In FIG. 6A, at step 605, the monitoring apparatus receives a message from a probe. At step 610, the metric is determined from the message. At step 615, a value for the metric is determined. At step 620, a site for the probe is determined.

At step 625 (FIG. 6B), the monitoring apparatus determines if the metric is site-specific. If the metric is site specific, then at step 630 the monitoring apparatus determines an acceptable value or range of values for the metric/site combination. Otherwise, at step 635, the monitoring apparatus determines an acceptable value or range of values for the metric, without regard to the site of the probe. Either way, at step 640, the system compares the value from the message with the acceptable value/range.

At step 645 (FIG. 6C), the monitoring apparatus determines if the value for the metric is acceptable. If the value is acceptable, then at step 650 the monitoring apparatus logs the value for the metric and the site from which the value was received. Otherwise, at step 655, the monitoring apparatus displays an alert, letting someone know about a potential problem.

As shown in FIG. 6A, certain steps can be omitted or repeated. For example, since a single message can include values for multiple metrics, steps 610 and 615 can be repeated. Also, if the metrics are not site-specific, step 620 can be omitted (although typically the site is transmitted as part of the message, even if the metric is not site-specific). Finally, as shown on FIG. 6C, if the value for the metric is acceptable, the value does not need to be logged, although, again, typically the value is logged.

A person skilled in the art will recognize that an embodiment of the invention described above can be implemented using a computer. In that case, the method is embodied as instructions that make up a program. The program may be stored on computer-readable media, such as floppy disks, optical discs (such as compact discs), or fixed disks (such as hard drives), and can be resident in memory, such as random access memory (RAM), read-only memory (ROM), firmware, or flash RAM memory. The program as software can then be executed on a computer to implement the method. The program, or portions of its execution, can be distributed over multiple computers in a network.

Having illustrated and described the principles of the invention in a preferred embodiment thereof, it should be readily apparent to those skilled in the art that the invention

can be modified in arrangement and detail without departing from such principles. All modifications coming within the spirit and scope of the accompanying claims are claimed.

CLAIMS

1. A probe apparatus comprising:

a first sensor to capture a first value for a first metric on a computer; and

a message generator operative to send a first message to a central site, the message including the first value.

2. A probe apparatus according to claim 1, further comprising a second sensor to capture a second value for a second metric on the computer.

3. A probe apparatus according to claim 2, wherein the message generator is operative to send a second message to the central site, the second message including the second value.

4. A probe apparatus according to claim 2, wherein the message generator is operative to include the second value in the first message.

5. A probe apparatus according to claim 1, further comprising a timer, the first sensor operative to capture the first value for the first metric when the timer ends and to reset the timer.

6. A probe apparatus according to claim 1, wherein:

the computer includes a software package; and

the probe monitors the software package.

7. A probe apparatus according to claim 1, wherein:

the computer includes a database; and

the probe monitors the database.

8. A monitoring apparatus, the system comprising:

a message receiver to receive a first message from a first site, the first message including a first value for a first metric;

a tester to determine if the first value is acceptable; and

an alerter to alert someone if the first value is not acceptable.

9. A monitoring apparatus according to claim 8, wherein:

the tester includes a first filter, the first filter defining a range of acceptable values for the first metric; and

the tester is operative to compare the first value with the range of acceptable values for the first filter.

10. A monitoring apparatus according to claim 9, wherein the tester includes:

a plurality of filters, each filter determining a range of acceptable values for a metric; and

a selector to select the first filter from the plurality of filters based on the first metric in the first message.

11. A monitoring apparatus according to claim 10, wherein:

the plurality of filters includes at least one filter defining a range of acceptable values for the first metric associated with a site; and

a selector to select the first filter from the plurality of filters based on a first site in the first message.

12. A monitoring apparatus according to claim 8, further comprising a log, the log including an entry corresponding to the first message.

13. A system for monitoring software, comprising:

a central computer;

a monitoring apparatus installed in the central computer;

a first computer;

a first probe installed in the first computer; and

a network connecting the central computer and the first computer.

14. A system according to claim 13, where:

the system further comprises:

a second computer; and

a second probe installed in the second computer; and

the network connects the central computer and the second computer.

15. A system according to claim 13, wherein:
the first computer includes a software package; and
the first probe monitors the software package.

16. A system according to claim 13, wherein:
the first computer includes a database; and
the first probe monitors the database.

17. A system according to claim 13, wherein:
the monitoring apparatus includes:
a message receiver to receive a first message from a first site, the first message including a first value for a first metric;
a tester to determine if the first value is acceptable; and
an alerter to alert someone if the first value is not acceptable; and
the probe includes:
a first sensor to capture a first value for a first metric; and
a message generator operative to send a first message to a central site, the message including the first value.

18. A system according to claim 13, wherein the first computer includes an e-mail server to generate a message from the first probe to the monitoring apparatus.

19. A method for using a probe, comprising:
accessing a first value for a first metric by the probe;
generating a message by the probe, the message including the first value for the first metric; and
sending the message to a monitoring apparatus by the probe.

20. A method according to claim 19, wherein sending the message includes:
delivering the message to an e-mail server by the probe;
delivering the message to the monitoring apparatus by the e-mail server.

21. A method according to claim 19, wherein accessing the first value includes accessing a software package by the probe.

22. A method according to claim 19, wherein accessing the first value includes accessing a database by the probe.

23. A method according to claim 19, wherein generating a message further includes generating the message by the probe, the message including the first value for the first metric and an identifier for a site of the probe.

24. A method for using a monitoring apparatus, comprising:

receiving a message;

determining a first value for a first metric from the message;

determining if the first value for the first metric is acceptable; and

if the first value for the first metric is not acceptable, displaying an alert that the first value for the first metric is not acceptable.

25. A method according to claim 24, further comprising, if the first value for the first metric is acceptable, logging the first value for the first metric.

26. A method according to claim 24, wherein:

determining a first value includes determining the first value for the first metric for a first site from the message; and

determining if the first value for the first metric is acceptable includes determining if the first value for the first metric for the first site is acceptable.

27. A method according to claim 24, wherein determining if the first value for the first metric is acceptable includes comparing the first value for the first metric with at least one acceptable value.

28. A method according to claim 24, wherein determining if the first value for the first metric is acceptable includes determining if the first value for the first metric is within a range of acceptable values.

29. A method according to claim 24, wherein receiving a message includes:
accessing the first value for the first metric by a probe;
generating the message by the probe; and
sending the message to the monitoring apparatus by the probe.

30. A method according to claim 29, wherein sending the message includes:
delivering the message to an e-mail server by the probe;
delivering the message to the monitoring apparatus by the e-mail server.

31. A method according to claim 29, wherein accessing the first value includes accessing a software package by the probe.

32. A method according to claim 29, wherein accessing the first value includes accessing a database by the probe.

33. A method according to claim 29, wherein generating a message further includes generating the message by the probe, the message including the first value for the first metric and an identifier for a site of the probe.

34. Computer-readable media containing a program to use a probe, the program comprising:
software to access a first value for a first metric by the probe;
software to generate a message by the probe, the message including the first value for the first metric; and
software to send the message to a monitoring apparatus by the probe.

35. Computer-readable media according to claim 34, wherein the software to send the message includes:
software to deliver the message to an e-mail server by the probe;

software to deliver the message to the monitoring apparatus by the e-mail server.

36. Computer-readable media according to claim 34, wherein the software to access the first value includes software to access a software package by the probe.

37. Computer-readable media according to claim 34, wherein the software to access the first value includes software to access a database by the probe.

38. Computer-readable media according to claim 19, wherein the software to generate a message further includes software to generate the message by the probe, the message including the first value for the first metric and an identifier for a site of the probe.

39. Computer-readable media containing a program to use a monitoring apparatus, the program comprising:

software to receive a message;

software to determine a first value for a first metric from the message;

software to determine if the first value for the first metric is acceptable; and

if the first value for the first metric is not acceptable, software to display an alert that the first value for the first metric is not acceptable.

40. Computer-readable media according to claim 39, further comprising, if the first value for the first metric is acceptable, software to log the first value for the first metric.

41. Computer-readable media according to claim 39, wherein:

the software to determine a first value includes software to determine the first value for the first metric for a first site from the message; and

the software to determine if the first value for the first metric is acceptable includes software to determine if the first value for the first metric for the first site is acceptable.

42. Computer-readable media according to claim 39, wherein the software to determine if the first value for the first metric is acceptable includes software to compare the first value for the first metric with at least one acceptable value.

43. Computer-readable media according to claim 39, wherein the software to determine if the first value for the first metric is acceptable includes software to determine if the first value for the first metric is within a range of acceptable values.

44. Computer-readable media according to claim 39, wherein the software to receive a message includes:

software to access the first value for the first metric by a probe;

software to generate the message by the probe; and

software to send the message to the monitoring apparatus by the probe.

45. Computer-readable media according to claim 44, wherein the software to send the message includes:

software to deliver the message to an e-mail server by the probe;

software to deliver the message to the monitoring apparatus by the e-mail server.

46. Computer-readable media according to claim 44, wherein the software to access the first value includes software to access a software package by the probe.

47. Computer-readable media according to claim 44, wherein the software to access the first value includes software to access a database by the probe.

48. Computer-readable media according to claim 44, wherein the software to generate a message further includes software to generate the message by the probe, the message including the first value for the first metric and an identifier for a site of the probe.

49. A probe apparatus substan tially as herein described and illustrated.

50. A monitoring as herein described and illustrated.

51. A system for monitoring software substantially as herein described and illustrated.

52. A system for using a probe substantially as herein described and illustrated.

53. A method for using a monitoring apparatus substantially as herein described and illustrated.

54. A computer-readable media substantially as herein described and illustrated.

DATED THIS 16TH DAY OF SEPTEMBER 2004

SPOOR & FISHER
APPLICANTS PATENT ATTORNEYS

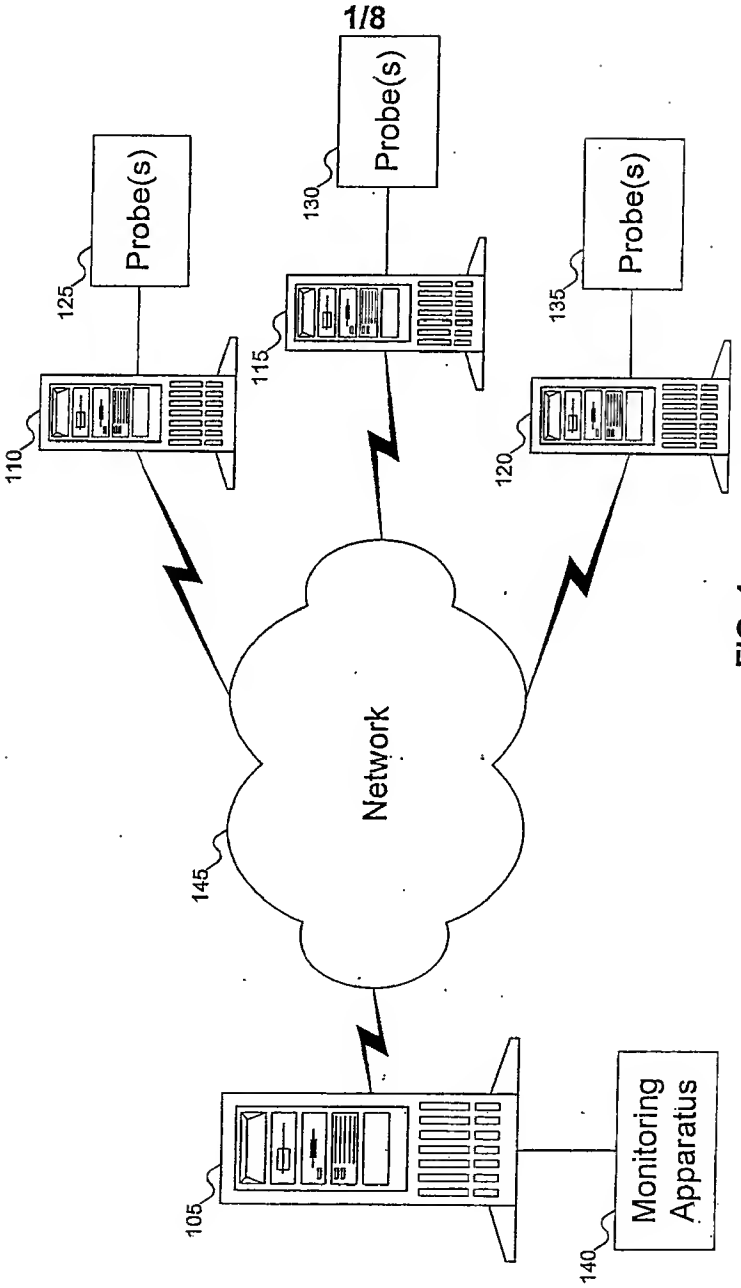
Probe(s)
125
Probe(s)
130
Probe(s)
135
110
115
120
Network
145
105
Monitoring Apparatus
140

FIG. 1

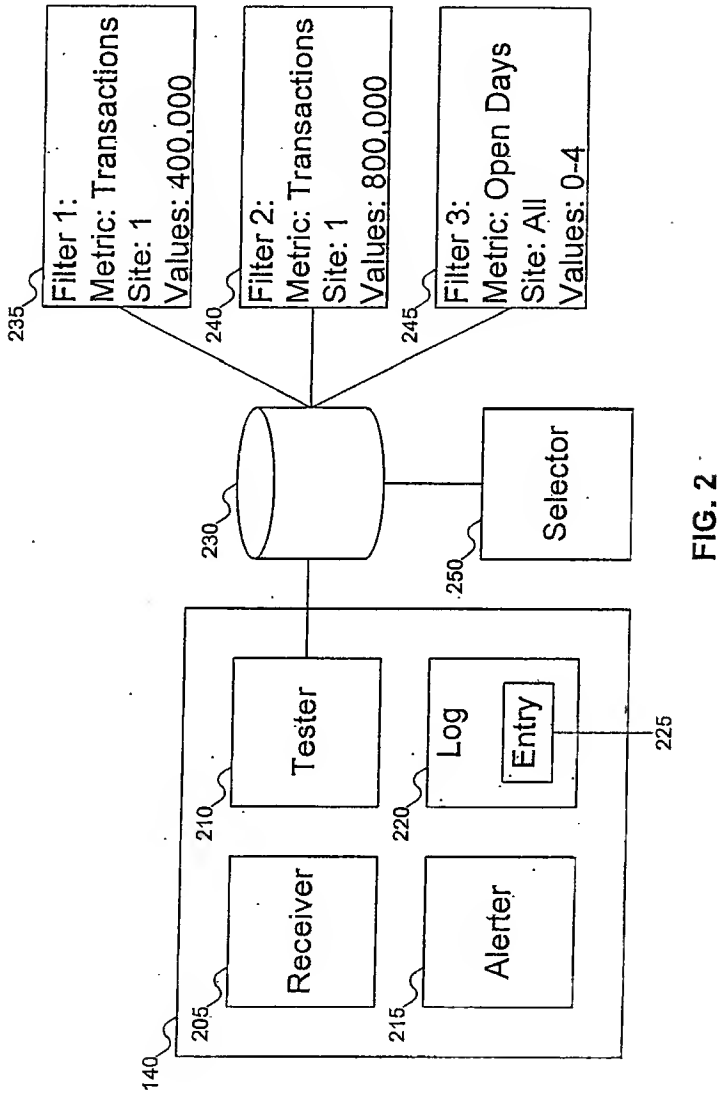
Filter 1:
Metric: Transactions
Site: 1
Values: 400,000
235
Filter 2:
Metric: Transactions
Site: 1
Values: 800,000
240
Filter 3:
Metric: Open Days
Site: All
Values: 0-4
245
230
Selector
250
Tester
210
Log
Entry
220
225
Receiver
205
Alerter
215
140

FIG. 2

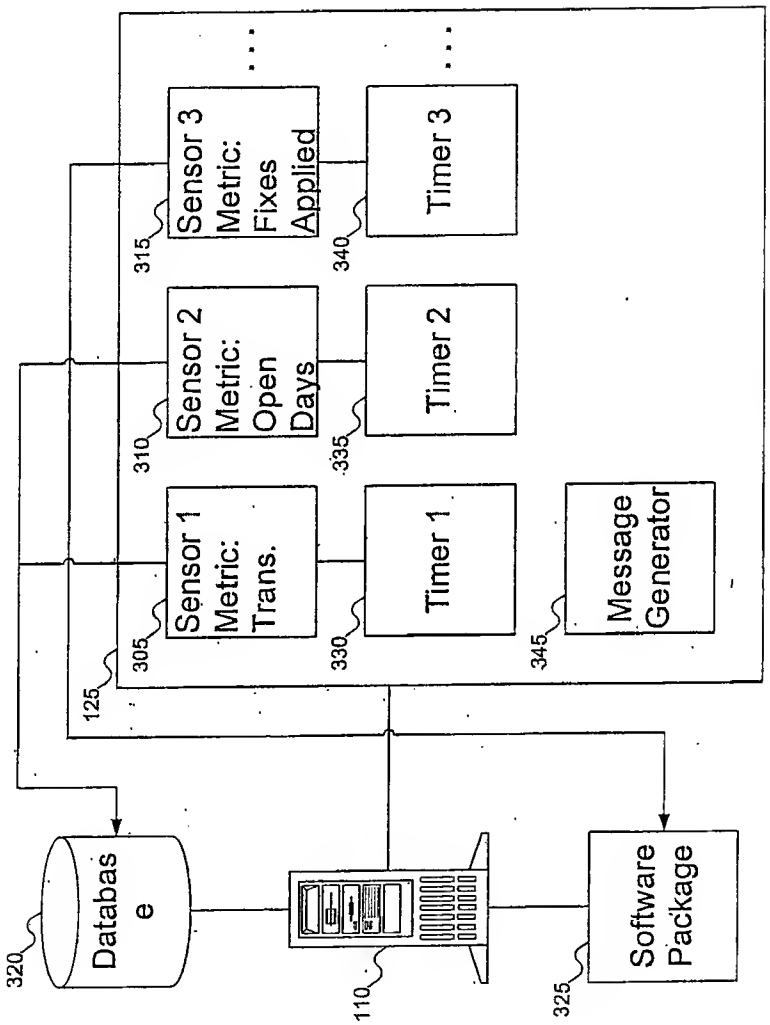
Sensor 3 Metric: Fixes Applied
Timer 3
Sensor 2 Metric: Open Days
Timer 2
Sensor 1 Metric: Trans.
Timer 1
Message Generator
315
340
310
335
305
330
345
125
Databas e
320
110
Software Package
325

FIG. 3

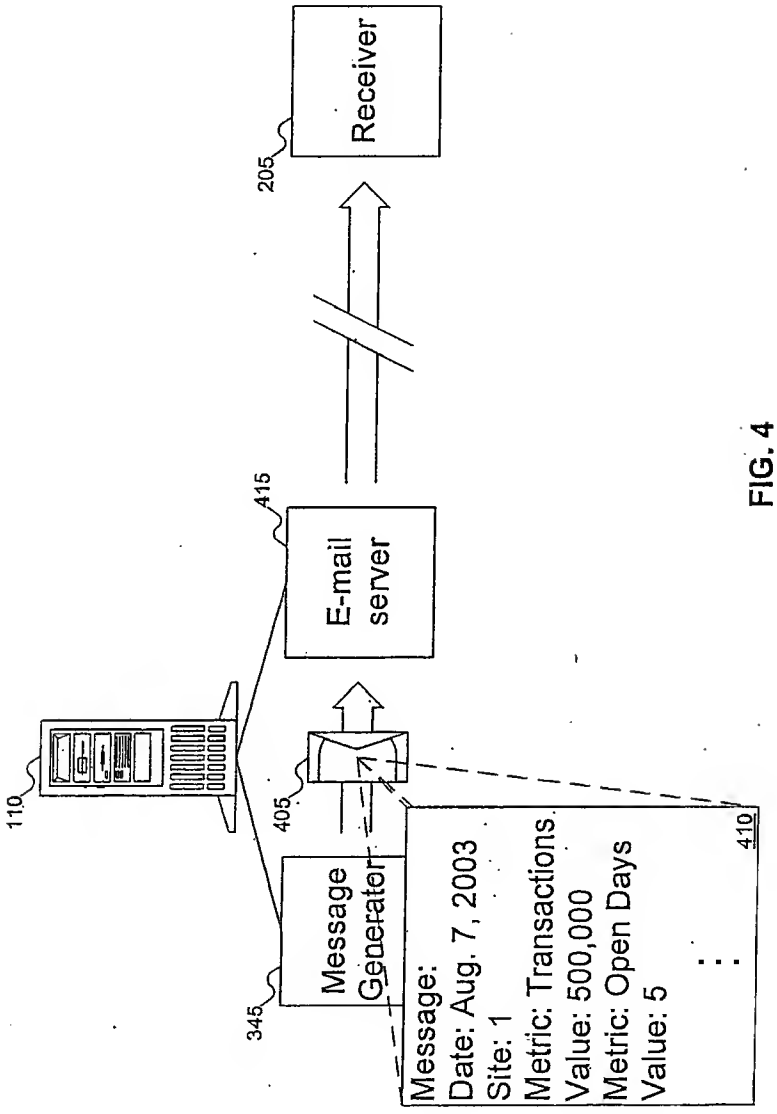
Receiver
205
E-mail server
415
110
405
Message Generator
345
Message:
Date: Aug. 7, 2003
Site: 1
Metric: Transactions
Value: 500,000
Metric: Open Days
Value: 5
410

FIG. 4

5/8

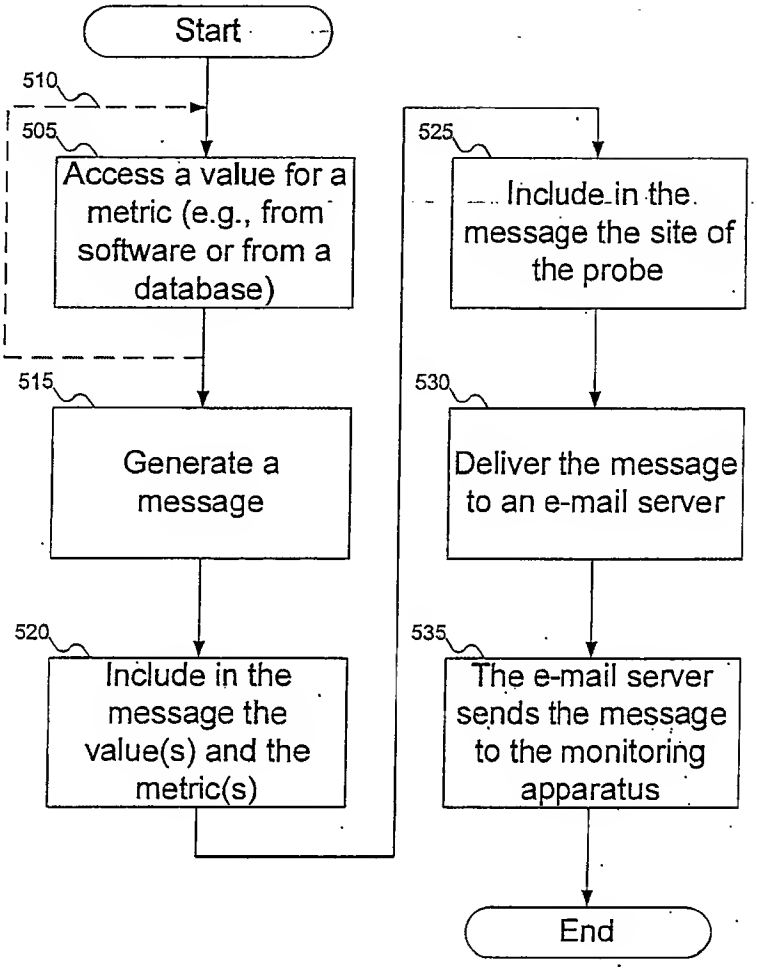
Start
510
505
Access a value for a metric (e.g., from software or from a database)
515
Generate a message
520
Include in the message the value(s) and the metric(s)
525
Include in the message the site of the probe
530
Deliver the message to an e-mail server
535
The e-mail server sends the message to the monitoring apparatus
End

FIG. 5

6/8

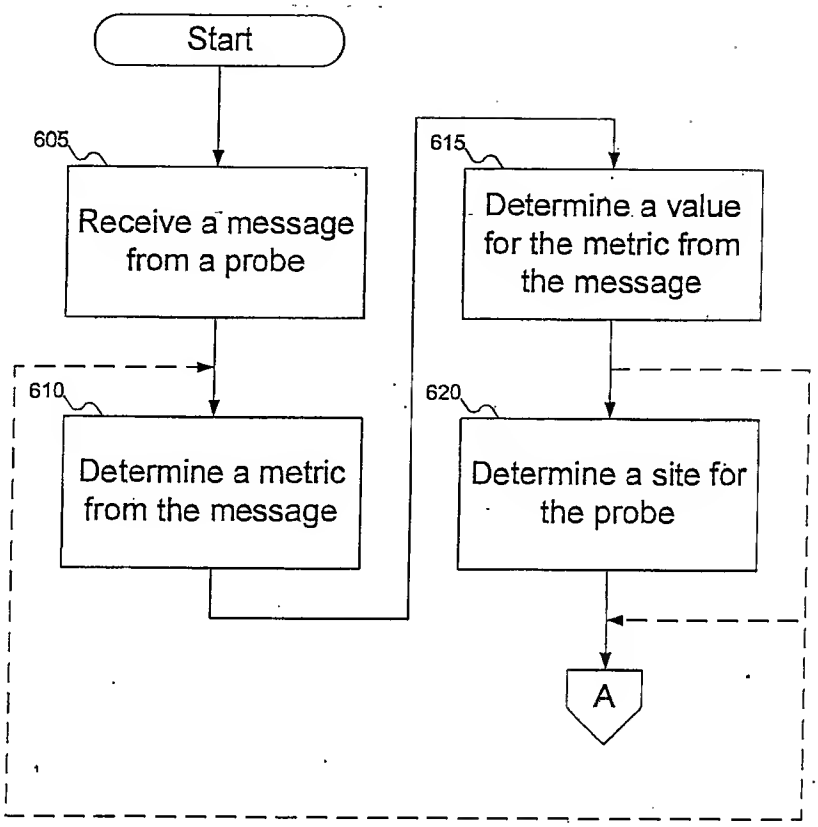
Start
605
Receive a message from a probe
610
Determine a metric from the message
615
Determine a value for the metric from the message
620
Determine a site for the probe
A

FIG. 6A

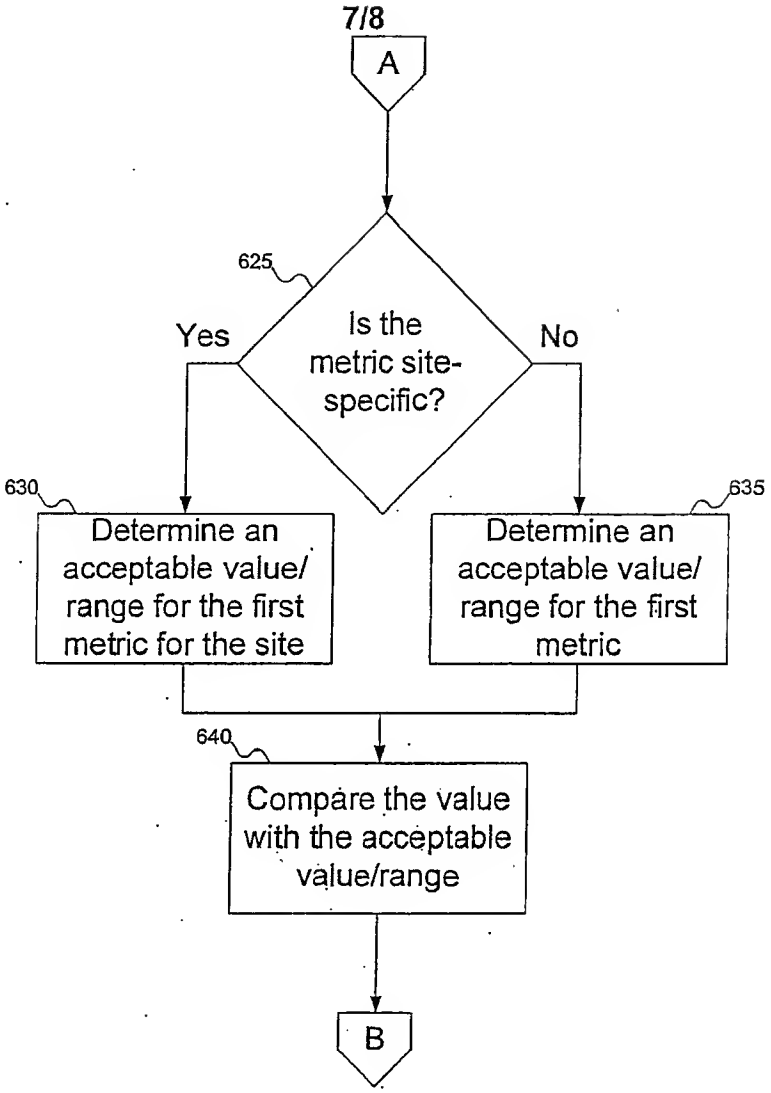
7/8
A
625
Is the metric site-specific?
Yes
No
630
Determine an acceptable value/ range for the first metric for the site
635
Determine an acceptable value/ range for the first metric
640
Compare the value with the acceptable value/range
B

FIG. 6B

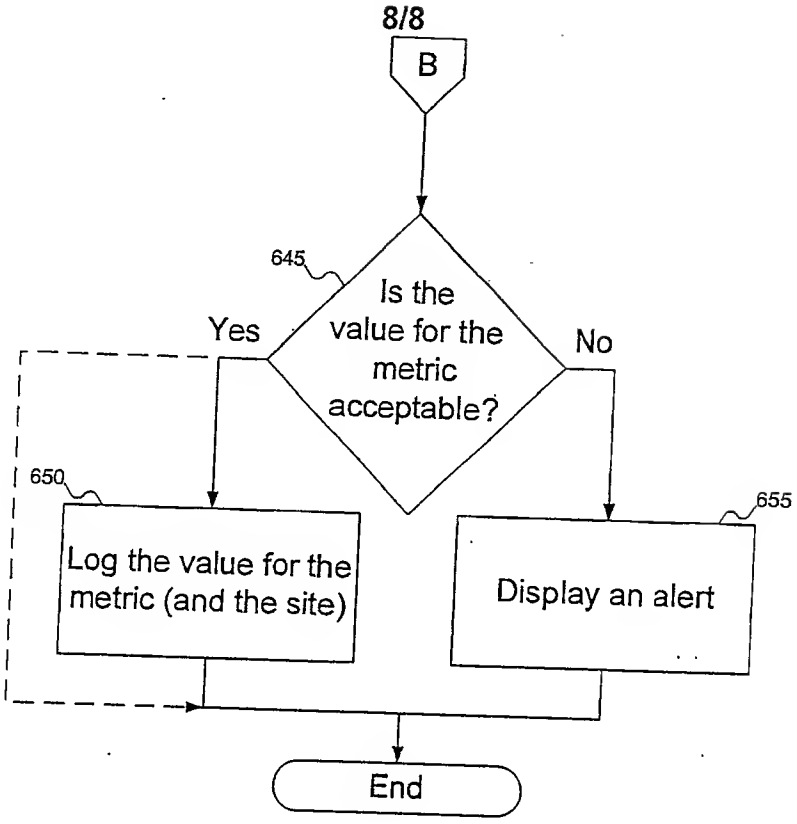
8/8
B
645
Is the value for the metric acceptable?
Yes
No
650
Log the value for the metric (and the site)
655
Display an alert
End

FIG. 6C